DAILY SCIENCE
DÉCOUVREZ LA SCIENCE, LA RECHERCHE ET L'INNOVATION "MADE IN BELGIUM"

LA CONFIDENTIALITÉ SUR INTERNET N'EXISTE PAS

Publié le 6 février 2019

par Christian Du Brulle

Mauvaise nouvelle. Mots de passe, clés de cryptage, codes secrets de toutes sortes: vous pensiez que vos messages, vos photos de vacances, mais aussi vos informations plus personnelles transmises ou stockées sur internet étaient sûres et confidentielles? Vous vous trompez! Vos données sont absolument transparentes. Ou du moins, elles le seront dans un proche avenir.

Voilà en substance le message (non codé!) que distille ces jours-ci à Bruxelles, au Collège Belgique, le Québécois Gilles Brassard.

« Rien de ce que vous confiez en ligne n'est sûr », explique ce professeur au Département d'informatique et de recherche opérationnelle de l'Université de Montréal. « Ou plus exactement, rien de ce que vous avez confié ou transmis jusqu'à présent, et ce depuis les débuts de l'internet, n'est confidentiel ».

Un jeu d'enfant pour l'ordinateur quantique

Et le chercheur ne parle pas ici de ce que vous rendez public sur les réseaux sociaux. Il pense à vos données sensibles, par exemple celles liées à votre santé. Des informations que vous n'aimeriez pas voir tomber entre les mains de compagnies d'assurances par exemple.

« Bien sûr, les méthodes de cryptage et autres moyens destinés à rendre l'information opaque aux

yeux des personnes qui ne doivent pas y avoir accès sont aujourd'hui relativement efficaces », souligne en substance cet informaticien, lauréat du Prix Wolf de physique en 2018 pour ses travaux théoriques en cryptographie quantique. « Mais il suffit pour un Etat ou une importante entreprise d'intercepter vos données cryptées, de les stocker et d'attendre pour pouvoir en prendre un jour connaissance avec facilité ».

Vulnérabilité rétroactive

La clé de cette déconcertante facilité de lecture des secrets les mieux gardés porte un nom: l'ordinateur quantique. Cette machine, qui est peut-être déjà une réalité dans une cave bien gardée ou au coeur d'un centre de recherche discret, se joue des méthodes de cryptographie classique. Sa puissance de calcul est (sera) telle que rien ne lui résistera. Tout ce qui aura été crypté jusque là lui sera transparent. « C'est aussi simple que cela », estime l'informaticien.

« L'informatique quantique est au confluent de l'informatique, des mathématiques et de la physique », précise Gilles Brassard. Elle s'intéresse à toutes les façons par lesquelles les propriétés parfois déroutantes de la mécanique quantique peuvent améliorer notre capacité de traiter l'information, ce qui permet en principe de faire des calculs qui semblent hors de portée des ordinateurs conventionnels ».

Science-fiction? "L'industrie investit actuellement des milliards de dollars dans les technologies quantiques", souligne le Pr Brassard. "En Chine, un programme de recherche spécifiquement dédié à cette branche est doté de douze milliards de dollars. Et cela, c'est ce que l'on connaît…"

Deux voies d'avenir pour une meilleure sécurisation

Une parade est-elle envisageable? Pour tout ce qui a été codé jusqu'à présent, la réponse est clairement négative.

« Pour l'avenir, j'identifie deux voies », reprend le Pr Brassard. "Développer plusieurs nouvelles infrastructures cryptographiques post-quantiques". Diverses initiatives dans le monde seraient en cours de développement. "Cela va à terme impliquer que nous modifions toute l'infrastructure existante, y compris logicielles. Cela prendra du temps. Cela va coûter cher. Mais ce sera toujours moins cher que si nous ne faisions rien. C'est comme pour les changements climatiques. Si on ne fait rien, on va dans le mur…"

"La seconde option fait appel à la cryptographie quantique. Il s'agit d'utiliser les propriétés de la physique quantique pour rendre la confidentialité des échanges réellement invulnérables, même pour un ordinateur quantique », conclut le Pr Brassard.

Rendez-vous au Collège Belgique

Le Pr Gilles Brassard détaillera ces concepts lors de la première de ses deux leçons publiques données dans la cadre de la Chaire du Québec, jeudi soir à Bruxelles. Intitulée « L'art du secret dans un monde quantique », cette leçon de deux heures est accessible gratuitement (sur inscription toutefois).

Le lendemain, Gilles Brassard donnera une seconde leçon dans le cadre de cette Chaire du Québec. Toujours au palais des Académies, cette seconde intervention traitera de « Einstein et l'action fantomatique à distance ».

La « Chaire du Québec » bénéficie du soutien et de la coopération de la Délégation générale du Québec à Bruxelles.

DAILY SCIENCE
DÉCOUVREZ LA SCIENCE, LA RECHERCHE ET L'INNOVATION "MADE IN BELGIUM"